

U.S. Court Orders NSO Group to Hand Over Pegasus Spyware Code to WhatsApp

Mar 02, 2024 Newsroom : 4-5 minutes

A U.S. judge has ordered NSO Group to hand over its source code for [Pegasus](#) and other products to Meta as part of the social media giant's ongoing litigation against the Israeli spyware vendor.

The [decision](#), which marks a major legal victory for Meta, which [filed the lawsuit](#) in October 2019 for using its infrastructure to [distribute the spyware](#) to approximately 1,400 mobile devices between April and May. This also [included](#) two dozen Indian activists and journalists.

These attacks leveraged a then zero-day flaw in the instant messaging app ([CVE-2019-3568](#), CVSS score: 9.8), a critical [buffer overflow bug](#) in the voice call functionality, to deliver Pegasus by merely placing a call, even in scenarios where the calls were left unanswered.

In addition, the attack chain included steps to erase the incoming call information from the logs in an attempt to sidestep detection.

Court documents released late last month show that NSO Group has been asked to "produce information concerning the full functionality of the relevant spyware," specifically for a period of one year before the alleged attack to one year after the alleged attack (i.e., from April 29, 2018 to May 10, 2020).

That said, the company doesn't have to "provide specific information regarding the server architecture at this time" because WhatsApp "would be able to glean the same information from the full functionality of the alleged spyware." Perhaps more significantly, it has been spared from sharing the identities of its clientele.

"While the court's decision is a positive development, it is disappointing that NSO Group will be allowed to continue keeping the identity of its clients, who are responsible for this unlawful targeting, secret," [said](#) Donncha Ó Cearbhaill, head of the Security Lab at Amnesty International.

NSO Group was [sanctioned](#) by the U.S. in 2021 for developing and supplying cyber weapons to foreign governments that "used these tools to maliciously target government officials, journalists, businesspeople, activists, academics, and embassy workers."

Meta, however, is [facing mounting scrutiny](#) from privacy and consumer groups in the European Union over its "pay or okay" (aka pay or consent) [subscription model](#), which they say is a Hobson's choice between paying a "privacy fee" and consenting to be tracked by the company.


"This imposes a business model in which privacy becomes a luxury rather than a fundamental right, directly reinforcing existing discriminatory exclusion from access to the digital realm and control over personal data," they said, adding the practice would undermine GDPR regulations.

The development comes as Recorded Future revealed a new multi-tiered delivery infrastructure associated with [Predator](#), a mercenary mobile spyware managed by the Intellexa Alliance.

The infrastructure network is highly likely associated with Predator customers, including in countries like Angola, Armenia, Botswana, Egypt, Indonesia, Kazakhstan, Mongolia, Oman, the Philippines, Saudi Arabia, and Trinidad and Tobago. It's worth noting that no Predator customers within Botswana and the Philippines had been identified until now.

"Although Predator operators respond to public reporting by altering certain aspects of their infrastructure, they seem to persist with minimal alterations to their modes of operation; these include consistent spoofing themes and focus on types of organizations, such as news outlets, while adhering to established infrastructure setups," the company [said](#).

Sekoia, in its own [report](#) about the Predator spyware ecosystem, said it found three domains related to customers in Botswana, Mongolia, and Sudan, stating it detected a "significant increase in the number of generic malicious domains which do not give indications on targeted entities and possible customers."

Found this article interesting? Follow us on [Twitter](#)  and [LinkedIn](#) to read more exclusive content we post.